§170.315(g)(10) Standardized API for patient and population services

2015 Edition Cures Update CCG

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	06-15-2020

Regulation Text

Regulation Text

§ 170.315(g)(10) *Standardized API for patient and population services*—

The following technical outcomes and conditions must be met through the demonstration of application programming interface technology.

(i) *Data response.*

(A) Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 170.215(a)(2), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(B) Respond to requests for multiple patients' data as a group according to the standard adopted in § 170.215(a)(1), and implementation specifications adopted in § 170.215(a)(2) and (4), for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

(ii) *Supported search operations.*

(A) Respond to search requests for a single patient's data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(2), specifically the mandatory capabilities described in "US Core Server CapabilityStatement".

(B) Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

(iii) *Application registration.* Enable an application to register with the Health IT Module's "authorization server."

(iv) *Secure connection.*

(A) Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(a)(2) and (3).

(B) Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(a)(4).

(v) *Authentication and authorization.*

(A) *Authentication and authorization for patient and user scopes.*

(1) First time connections.

(i) Authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b).

(ii) An application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months.

(2) Subsequent connections.

(i) Access must be granted to patient data in accordance with the implementation specification adopted in§ 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application.

(ii) An application capable of storing a client secret must be issued a new refresh token valid for a new period of no less than three months.

(B) *Authentication and authorization for system scopes.* Authentication and authorization must occur during the process of granting an application access to patient data in accordance with the "SMART Backend Services: Authorization Guide" section of the implementation specification adopted in § 170.215(a)(4) and the application must be issued a valid access token.

(vi) *Patient authorization revocation.* A Health IT Module's authorization server must be able to revoke an authorized application's access at a patient's direction.

(vii) *Token introspection.* A Health IT Module's authorization server must be able to receive and validate tokens it has issued.

(viii) *Documentation.*

(A) The API(s) must include complete accompanying documentation that contains, at a minimum:

(1) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns.

(2) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s).

(3) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

(B) The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

Standard(s) Referenced

Paragraph (g)(10)(i)(A)

§ 170.215(a)(1) Health Level 7 (HL7®) Version 4.0.1 Fast Healthcare Interoperability Resources Specification (FHIR®) Release 4, October 30, 2019

§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.0

§ 170.213 United States Core Data for Interoperability (USCDI)

Paragraph (g)(10)(i)(B)

§ 170.215(a)(1) *HL7® Version 4.0.1 FHIR® Release 4, October 30, 2019*

§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.0

§ 170.213 USCDI

§ 170.215(a)(4) HL7® FHIR Bulk Data Access (Flat FHIR) (V1.0.0:STU 1)

Paragraph (g)(10)(ii)(A)

§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.0

Paragraph (g)(10)(ii)(B)

§ 170.215(a)(4) HL7® FHIR® Bulk Data Access (Flat FHIR®) (V1.0.0:STU 1)

Paragraph (g)(10)(iii)

None

Paragraph (g)(10)(iv)(A)

§ 170.215(a)(2) FHIR® US Core Implementation Guide STU V3.1.0

§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0

Paragraph (g)(10)(iv)(B)

§ 170.215(a)(4) HL7® FHIR Bulk Data Access (Flat FHIR) (V1.0.0:STU 1)

Paragraph (g)(10)(v)(A)(1)

§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0

§ 170.215(b) OpenID Connect Core 1.0 incorporating errata set 1

Paragraph (g)(10)(v)(A)(2)

§ 170.215(a)(3) HL7® SMART Application Launch Framework Implementation Guide Release 1.0.0

Paragraph (g)(10)(v)(B)

§ 170.215(a)(4) HL7® FHIR Bulk Data Access (Flat FHIR) (V1.0.0:STU 1)

Paragraph (g)(10)(vi)

None

Paragraph (g)(10)(vii)

None

Paragraph (g)(10)(viii)

None

Certification Companion Guide: Standardized API for patient and population services

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule). It includes extracts of preamble and regulation text from the ONC Cures Act Final Rule with accompanying clarifying interpretations. To access the full context of regulatory intent please consult the ONC Cures Act Final Rule or other included regulatory reference. This CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Included	Yes

Certification Requirements

Privacy and Security: This certification criterion was adopted in § 170.315(g)(10). As a result, an ONC-ACB must ensure that a product presented for certification to this criterion includes the privacy and security criteria (adopted in § 170.315(d)) within the overall scope of the certificate issued to the product.

- The privacy and security criteria (adopted in § 170.315(d)) do not need to be explicitly tested with this specific criterion unless it is the only criterion for which certification is requested.
- As a general rule, a product presented for certification only needs to be tested once to each applicable privacy and security criterion (adopted in § 170.315(d)) so long as the health IT developer attests that such privacy and security capabilities apply to the full scope of capabilities included in the requested certification.

Table for Privacy and Security

- If choosing Approach 1:
  - Authentication, access control, and authorization (§ 170.315(d)(1))
  - Trusted connection (§ 170.315(d)(9))
  - Either Auditable events and tamper-resistance (§ 170.315(d)(2)) or Auditing actions on health information (§ 170.315(d)(10)).
  - Encrypt authentication credentials (§ 170.315(d)(12))
  - Multi-factor authentication (MFA) (§ 170.315(d)(13))
- If choosing Approach 2:
  - For each applicable P&S certification criterion not certified for Approach 1, the health IT developer may certify using system documentation which is sufficiently detailed to enable integration such that the Health IT Module has implemented service interfaces to access external services necessary to meet the requirements of the P&S certification criterion. Please see the ONC Cures Act Final Rule at 85 FR 25710 for additional clarification.

Design and Performance: The following design and performance certification criteria (adopted in § 170.315(g)) must also be certified in order for the product to be certified.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, when different QMS are used, each QMS needs to be separately identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

Table for Design and Performance

- Quality management system (§ 170.315(g)(4))
- Accessibility-centered design (§ 170.315(g)(5))

Technical Explanations and Clarifications

Applies to Entire Criterion

Clarifications:

- On May 2, 2022, the API certification criterion in § 170.315(g)(10) replaces the "application access—data category request" certification criterion (§ 170.315(g)(8)).
- Health IT Modules are not required to support patient-facing API-enabled "read" services for multiple patients for the purposes of this certification criterion.
- The clinical note text included in any of the notes described in the "Clinical Notes Guidance" section of the US Core IG adopted in § 170.215(a)(2) must be represented in a "plain text" form, and it would be unacceptable for the note text to be converted to another file or format (e.g., .docx, PDF) when it is provided as part of an API response. The intent of this policy is to prohibit Health IT Modules from converting clinical notes from a "machine readable" format to a non-"machine readable" format (e.g., PDF). Clinical note text that originates from outside Health IT Modules should be exchanged using its original format. Additionally, "plain text" does not necessarily mean the FHIR "contentType" "text/plain."

Paragraph (10)(i)(A)

Technical outcome – Respond to requests for a single patient's data according to the standard adopted in § 170.215(a)(1) and implementation specification adopted in § 170.215(a)(2), including the mandatory capabilities described in "US Core Server CapabilityStatement," for each of the data included in the standard adopted in § 170.213. All data elements indicated as "mandatory" and "must support" by the standards and implementation specifications must be supported.

Clarifications:

- All data elements and operations indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported and are in-scope for testing.
- We clarify that Health IT Modules must demonstrate support for “Encounter,” “Organization,” and “Practitioner” US Core IG FHIR Profiles and “Location,” “PractitionerRole,” and “RelatedPerson” FHIR resources during testing and certification. Health IT Modules must support these US Core Profiles / FHIR resources because they are included as “must support” data elements in US Core Profiles required by the United States Core Data for Interoperability (USCDI).

Paragraph (10)(i)(B)

Technical outcome – Respond to requests for multiple patients’ data as a group according to the standard adopted in § 170.215(a)(1), and implementation specifications adopted in § 170.215(a)(2) and (4), for each of the data included in the standard adopted in § 170.213. All data elements indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported.

Clarifications:

- Health IT Modules may support scopes using either “system/*.read” or a list of “system/[resource].read,” where [resource] is the FHIR resource name, to enable the export of multiple patients’ data as a group.
- During testing and certification, Health IT Modules must demonstrate support for “Encounter,” “Organization,” and “Practitioner” US Core IG FHIR Profiles and “Location,” “PractitionerRole,” and “RelatedPerson” FHIR resources for multiple patient services because these resources are included as “must support” data elements in US Core Profiles required by the USCDI.

Paragraph (10)(ii)(A)

Technical outcome – Respond to search requests for a single patient’s data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(2), specifically the mandatory capabilities described in “US Core Server CapabilityStatement”.

Clarifications:

- All data elements indicated as “mandatory” and “must support” by the standards and implementation specifications must be supported and are in scope for testing.
- For “Encounter,” “Organization,” and “Practitioner,” US Core profiles and “Location,” “PractitionerRole,” and “RelatedPerson” FHIR resources, only the “read” type interaction must be supported and will be included in testing and certification. The “search” type interactions for these profiles are not in scope for testing and certification.

Paragraph (10)(ii)(B)

Technical outcome – Respond to search requests for multiple patients' data consistent with the search criteria included in the implementation specification adopted in § 170.215(a)(4).

Clarifications:

- During testing and certification, Health IT Modules must demonstrate support for "Encounter," "Organization," and "Practitioner" US Core IG FHIR Profiles and "Location," "PractitionerRole," and "RelatedPerson" FHIR resources for multiple patient services because these resources are included as "must support" data elements in US Core Profiles required by the USCDI.

Paragraph (10)(iii)

Technical outcome – Enable an application to register with the Health IT Module's "authorization server."

Clarifications:

- Health IT presented for testing and certification must support app registration regardless of the scope of patient search utilized by the application (e.g. single or multiple).
- This certification criterion requires a health IT developer, as finalized in the Condition of Certification requirements, to demonstrate its registration process, but does not require conformance to a standard.
- The third-party application registration process that a health IT developer must meet under this criterion is not a form of review or "vetting" for purposes of this criterion.

Paragraph (10)(iv)(A)

Technical outcome – Establish a secure and trusted connection with an application that requests data for patient and user scopes in accordance with the implementation specifications adopted in § 170.215(a)(2) and (3).

Clarifications:

- Connections below TLS version 1.2 must be denied.

Paragraph (10)(iv)(B)

Technical outcome – Establish a secure and trusted connection with an application that requests data for system scopes in accordance with the implementation specification adopted in § 170.215(a)(4).

Clarifications:

- Connections below TLS version 1.2 must be denied.

Paragraph (10)(v)(A)(*1*)

Technical outcome – For first time connections, authentication and authorization must occur during the process of granting access to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) and standard adopted in § 170.215(b). Additionally, an application capable of storing a client secret must be issued a refresh token valid for a period of no less than three months.

Clarifications:

- Health IT Modules will be explicitly tested for US Core IG operations using authentication and authorization tokens acquired via the process described in the implementation specification adopted in § 170.215(a)(3).
- Only the relevant parts of the OpenID Connect Core 1.0 including errata set 1 adopted in § 170.215(b) that are also included in the implementation specification adopted in § 170.215(a)(3) will be in-scope for testing and certification.
- We explicitly require mandatory support of the “SMART on FHIR Core Capabilities” in § 170.215(a)(3) because these capabilities are indicated as optional in the implementation specification. We further clarify these “SMART on FHIR Core Capabilities” are in scope for ONC Certification Program testing and certification.
- We clarify that by requiring the “permission-patient” “SMART on FHIR Core Capability” in § 170.215(a)(3), Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their electronic health information (EHI) based on FHIR resource-level scopes. Specifically, this means patients would need to have the ability to authorize access to their EHI at the individual FHIR resource level, from one specific FHIR resource (e.g., “Immunization”) up to all FHIR resources necessary to implement the standard adopted in § 170.213 and implementation specification adopted in § 170.215(a)(2).
- We clarify that Health IT Modules must demonstrate support for “Encounter,” “Location,” “Organization,” “Practitioner,” “PractitionerRole,” and “RelatedPerson” scopes during testing and certification. Health IT Modules must support these scopes because they are included as “must support” data elements in US Core Profiles required by the USCDI.
- Although Health IT Modules presented for testing and certification must include the ability for patients to authorize an application to receive their EHI based on FHIR resource-level scopes, Health IT Modules are not prohibited from presenting authorization scopes in a more user-friendly format (e.g. grouping resources under categories, renaming the scopes for easier comprehension by the end-user, using more granular scopes), as long as the ability for patients to authorize applications based on resource-level scopes is available, if requested by the patient.
- Implementers of § 170.315(g)(10)-certified Health IT Modules should be mindful of the information blocking provisions.

Paragraph (10)(v)(A)(*2*)

Technical outcome – For subsequent connections, access must be granted to patient data in accordance with the implementation specification adopted in § 170.215(a)(3) without requiring re-authorization and re-authentication when a valid refresh token is supplied by the application. Additionally, an application capable of storing a client secret must be issued a new refresh token valid for a new period of no less than three months.

Clarifications:

- No additional clarifications.

Paragraph (10)(v)(B)

Technical outcome – Authentication and authorization must occur during the process of granting an application access to patient data in accordance with the “SMART Backend Services: Authorization Guide” section of the implementation specification adopted in § 170.215(a)(4) and the application must be issued a valid access token.

Clarifications:

- No additional clarifications.

Paragraph (10)(vi)

Technical outcome – A Health IT Module’s authorization server must be able to revoke an authorized application’s access at a patient’s direction.

Clarifications:

- We have finalized this as a functional requirement to allow health IT developers the ability to implement it in a way that best suits their existing infrastructure and allows for innovative models for authorization revocation to develop.
- Patients are expected to have the ability to revoke an authorized application’s access to their EHI at any time.

Paragraph (10)(vii)

Technical outcome – A Health IT Module’s authorization server must be able to receive and validate tokens it has issued.

Clarifications:

- Although a standard for token introspection is not specified, we encourage industry to coalesce around using a common standard, like OAuth 2.0 Token Introspection (RFC 7662).

Paragraph (10)(viii)(A)

Technical outcome – The API(s) must include complete accompanying documentation that contains, at a minimum: (*1*) API syntax, function names, required and optional parameters supported and their data types, return variables and their types/structures, exceptions and exception handling methods and their returns; (*2*) The software components and configurations that would be necessary for an application to implement in order to be able to successfully interact with the API and process its response(s); and (*3*) All applicable technical requirements and attributes necessary for an application to be registered with a Health IT Module's authorization server.

Clarifications:

- Health IT developers are not required to re-publish documentation from the adopted standards and implementation specifications. However, health IT developers must publish documentation that goes beyond the adopted standards and implementation specifications.
- Health IT developers are expected to disclose any additional data their § 170.315(g)(10)-certified Health IT Module supports in the context of the adopted standards and implementation specifications.

Paragraph (10)(viii)(B)

Technical outcome – The documentation used to meet paragraph (g)(10)(viii)(A) of this section must be available via a publicly accessible hyperlink without any preconditions or additional steps.

Clarifications:

- No additional clarifications.

Content last reviewed on June 23, 2020